[redacted]

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIONRA TECHNOLOGIES LTD., *Plaintiff,* v. FORTINET, INC., *Defendant*	§ § § § § § § §	Case No. 2:22-cv-00322-JRG-RSP (LEAD CASE)
LIONRA TECHNOLOGIES LTD., *Plaintiff,* v. PALO ALTO NETWORKS, INC. *Defendant*	§ § § § § § § § § §	Case No. 2:22-cv-00334-JRG-RSP (Member Case) **JURY TRIAL DEMANDED**

DEFENDANT PALO ALTO NETWORKS, INC.'S
MOTION FOR SUMMARY JUDGMENT OF NON-INFRINGEMENT OF THE ASSERTED PATENTS

[redacted]

TABLE OF CONTENTS

[redacted]

TABLE OF AUTHORITES

Cases

Rules

[redacted]

I. INTRODUCTION

Lionra accuses Palo Alto Networks, Inc. ("PAN") of infringing claims 1, 2, 13, and 22 of U.S. Patent No. 7,685,436 (the "'436 Patent") and claims 1, 2, 12, and 13 of U.S. Patent No. 8,566,612 (the "'612 Patent") (collectively, the "Asserted Patents" and the "Asserted Claims"). Because the accused representative product, PA-5430 does not meet each and every claim limitation, there is no infringement for two distinct reasons: (1) the PA-5430's alleged packet engine does not operate on all incoming packets, as required; and (2) the PA-5430 is not configured to perform decryption as sold. For the avoidance of doubt, PAN moves for summary judgment of no direct or indirect infringement with respect to the first reason, and PAN moves for summary judgment of no direct infringement with respect the second reason.

All of the Asserted Claims are directed to a security processor that includes, *inter alia*, a switching system and packet engine(s). The Asserted Claims require that the security processor receive "incoming packets" via the switching system that "the incoming packets" must also be "received by the packet engine from the switching system," and further that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." '436 Patent, claims 1, 13; '612 Patent, claims 1, 13. During claim construction in this case, the Court addressed the meaning of the "substantially all" limitation. The Court explained that "[t]he claims require that the packet engines *operate on* 'the incoming packets,' **meaning all of them** and the "substantially all . . ." limitation expresses that not every packet *passes through* the packet engines." Claim Construction Order, Dkt. 162 at 33 (italics in original, bold emphasis added). Therefore, to show infringement, Lionra must show that all of "the incoming packets" to the accused switching system are processed by the accused packet engines. For purposes of trial and this motion, there is a single representative accused product: PA-5430

[redacted]

Next Generation Firewall (NGFW). Dkt. 204. The parties do not dispute the relevant features and operation of PA-5430, known internally as [redacted] which operation establishes the two independent reasons for non-infringement presented in this motion.

First (and with respect to both direct and indirect infringement), in a PA-5430, not all of the incoming packets to the accused switching system are received by the alleged "packet engines."

[redacted] As will be explained below and as the Court explained at claim construction, all Asserted Claims require that all incoming packets reach the packet engines. Because this does not happen in the accused PA-5430, the PA-5430 does not infringe any Asserted Claim.

Second (and only with respect to direct infringement by PAN) the PA-5430 does not directly infringe any Asserted Claim because each Asserted Claim requires a "cryptographic core" "configured to perform" "decryption" under the Court's construction (Dkt. 162; Asserted Patents, claims 1 and 13), and the PA-5430 is not configured as required to perform decryption when sold to customers. For this second reason, the undisputed facts warrant summary judgment of no direct infringement on all Asserted Claims.

II. SUMMARY JUDGMENT STANDARDS

Summary judgment should be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P.

56(a); *Celotex v. Catrett*, 477 U.S. 317, 322 (1986). "By its very terms, this standard provides that the mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no genuine [dispute] of material fact." *Anderson v. Liberty Lobby, Inc*., 477 U.S. 242, 247– 48 (1986). The substantive law identifies the material facts, and disputes over facts that are irrelevant or unnecessary will not defeat a motion for summary judgment. *Id*. at 248. A dispute about a material fact is "genuine" when the evidence is "such that a reasonable jury could return a verdict for the nonmoving party." *Id*.

The moving party must identify the basis for granting summary judgment and evidence demonstrating the absence of a genuine dispute of material fact. *Celotex*, 477 U.S. at 323. Where, as here, the moving party does not have the ultimate burden of persuasion at trial, the party "must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial." *Yufa v. TSI, Inc.*, 652 Fed. Appx. 939, 944 (Fed. Cir. 2016) (quoting *Nissan Fire & Marine Ins. Co., Ltd. v. Fritz Cos., Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000)). A party opposing a motion for summary judgment on a claim for which it carries the burden of proof must present evidence sufficient to prove each element of that claim in order to avoid summary judgment. *Celotex*, 477 U.S. at 322-23.

III. STATEMENT OF THE ISSUES

1. Whether the PA-5430 NGFW infringes the Asserted Claims requiring the packet engines to operate on all of "the incoming packets", where the facts and evidence are undisputed that the accused packet engines do not and cannot operate on all of the incoming packets since the packet engines in the PA-5430 do not receive all of the incoming packets.

[redacted]

2. Whether the PA-5430 NGFW directly infringes the Asserted Claims requiring a "cryptographic core . . . configured to perform . . . decryption," where the facts and evidence are undisputed that the PA-5430 as sold by PAN is not configured in a manner that even purportedly performs the required decryption in the cryptographic core.

IV. SUMMARY OF THE ALLEGED INVENTION

The '436 and '612 Patents are titled "System and Method for a Secure Interface." The '612 Patent, which is a continuation of the '436 Patent, shares the same specification and drawings used in the '436 Patent.[1] The Asserted Patents are directed to security processor systems configured to provide security and network processing to protect against unauthorized access or attack. '436 Patent, Abstract.

The Asserted Claims are directed to a security processor for processing data packets. '436 Patent, Abstract. The security processor includes a switching system (yellow), a cryptographic core (blue) and packet engines (green) interposed between the switching system and cryptographic cores. *Id*.

[1] Because the '436 and '612 Patents share a common specification, all citations are to the '436 Patent unless noted otherwise.

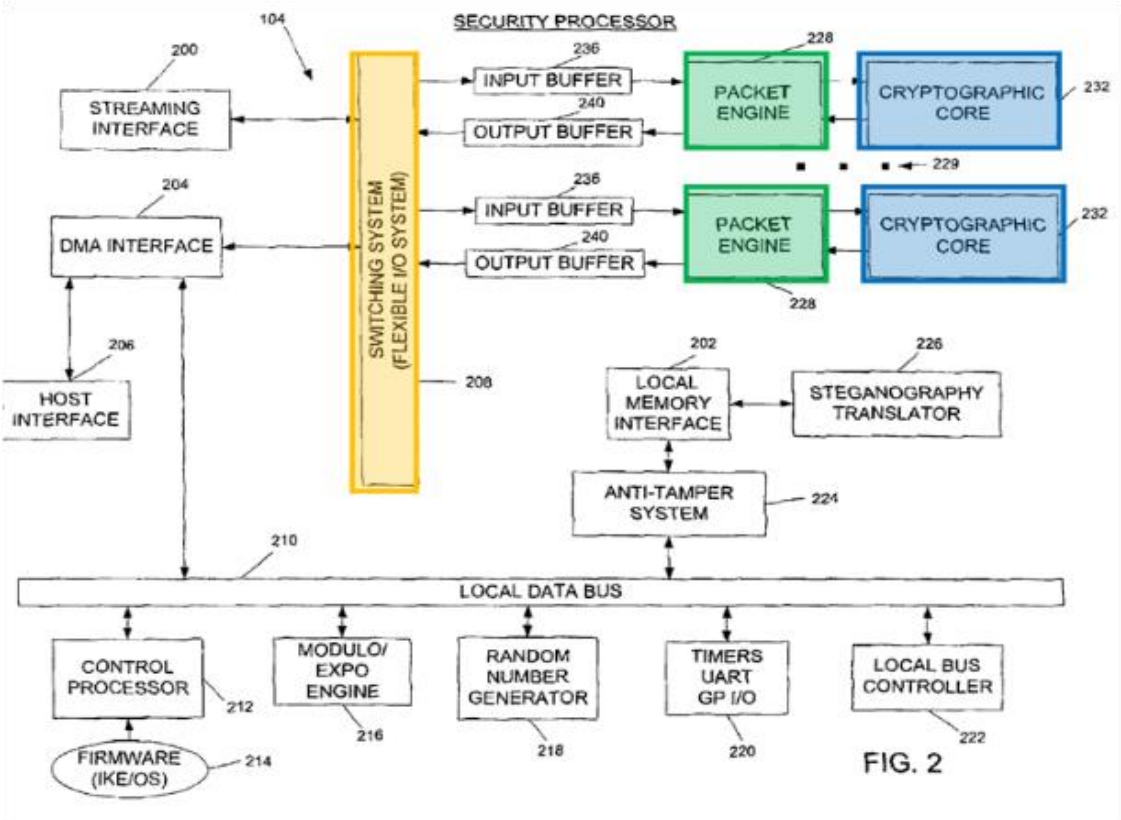


FIG. 2

'436 Patent, Fig. 2 (annotated).

In operation, the switching system provides a mechanism to route packets and data in the security processor. *Id.*, 6:58-61. The packet engines receive packets from the switching system and are used for packet processing and classification. *Id.*, 9:60-64, 10:8-13, 11:9-16, 20:4-14. The packet engine may forward the packets to other devices, such as a cryptographic core. *Id.*, 10:58-61, 11:11-16, 11:48-63, 20:8-14.

V. STATEMENT OF UNDISPUTED FACTS ("SOF")

1. PA-5430 NGFW running PAN-OS version 10.2 is, for purposes of this litigation, representative of all Accused Products. Dkt. 204.

2. PA-5430 runs the PAN-OS software on a

[redacted]

3. Lionra contends that the [redacted] core(s) and the software running on those cores comprise "a packet engine." [redacted]

4. PA-5430 also uses a [redacted]

5. Lionra contends that the [redacted] ethernet switch is the accused "switching system" of the claims. [redacted]

6. PA-5430 further includes [redacted]

[redacted]

[redacted]

7. Among other features, [redacted]

8. [redacted]

9. For a variety of reasons, not all packets sent to the firewall make it through the firewall. [redacted]

[redacted]

[redacted]

12. The Court entered the following claim constructions in this case for terms in the '436/'612 Patents:

[redacted]

- "The Court therefore hereby construes '**packet engine**' to mean '**hardware, or a combination of hardware and software, that is configured to perform packet operations**.'"

- "The Court therefore hereby construes '**cryptographic core**' to mean '**hardware, or a combination of hardware and software, that is configured to perform cryptographic processing.'"**

- **"**The Court accordingly hereby construes '**intrusion detection system**' to mean '**hardware, or a combination of hardware and software, that is configured for matching parts of a data stream against a stored set of patterns.'"**

Dkt. 162, at 39, 42, 46 (emphasis in original) (Judge Payne's Claim Construction Order dated November 27, 2023); Dkt. 190 (adopting same).

13. The PAN-OS Administrator's Guide produced in this case as PAN_00007717 et al. provides "Best Practices for Completing the Firewall Deployment" on page 62 which further provides: "Now that you have integrated the firewall into your network . . . you can begin configuring more advanced features" and identifies "Enable Decryption" as "some of the things to consider next." Ex. F, PAN-OS Administrator's Guide.

VI. ARGUMENT

A. In the Accused Products, the Alleged Packet Engine(s) Do Not Operate on All "Incoming Packets to the Security Processor" As Required By All Asserted Claims.

It is undisputed that in the PA-5430, incoming packets pass from [redacted] Only the remaining packets are sent to the [redacted] cores (the accused "packet engines"). As the Court explained at claim construction and further set forth below, the Asserted Claims require that all incoming packets must be received and operated on by the alleged packet engines. Because no reasonable juror could find that **all** of "the incoming packets" to the accused switching system are received by the

[redacted]

accused packet engine(s), no reasonable jury could find infringement and Palo Alto Networks is entitled to summary judgment in its favor.

1. The packet engines must operate on all of the incoming packets to the security processor for infringement.

The relevant claim requirements are the same in all four of the independent claims asserted. Independent claim 1 of the '612 patent is representative, reciting, in relevant part:

> 1. A security processor[2] to process incoming packets and outgoing packets, the security processor comprising:
> [1(a)] a switching system to send the outgoing packets and receive the incoming packets;
> [1(b)] a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines …;

Independent claim 13 of the '612 patent has identical requirements for the "incoming packets" as shown below:

> 13. A security processing system comprising:
> (a) a security processor comprising:
> [13(a)(i)] a switching system to send outgoing packets and to receive incoming packets;
> [13(a)(ii)] a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines;

Independent claims 1 and 13 of the '436 Patent identically recite the above emphasized elements.

Therefore, in summary form, the first two limitations of each Asserted Claim present the same requirements for the "incoming packets":

1. There is "[a] security processor" that processes "incoming packets";

[2] The parties agreed that the preamble language "security processor" is limiting" Dkt. 162 at 54.

2. "[T]he incoming packets" are received by "a switching system";
3. A packet engine is "coupled to the switching system";
4. "[T]he incoming packets" are "received by the packet engine from the switching system";
5. The packet engine is "one of a plurality of packet engines"; and
6. "[S]ubstantially all of the incoming… packets to the security processor transit one of the plurality of packet engines."

Most importantly for the present motion, every Asserted Claim requires "substantially all of **the incoming** and outgoing **packets to the security processor** transit one of the plurality of packet engines." *See e.g.,* '612 patent at claim [1(b)]. "The incoming packets" is an anaphoric phrase, referring back to the initial antecedent phrase. *See Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338 (Fed. Cir. 2008). In these claims, "the incoming … packets to the security processor" refers back to the "incoming packets" received by the switching system and also to "incoming packets" processed by the security processor. In other words, the same "incoming packets" that incoming to the security processor via the switching system must also be received by one of the plurality of packet engines under a plain reading of the claims. As this Court put succinctly during claim construction: "[t]he claims require that the packet engines *operate on* 'the incoming packets,' **meaning all of them**." Claim Construction Order, Dkt. 162 at 33 (italics in original; bold emphasis added). The Court further explained that "the "substantially all . . ." limitation expresses that not every packet *passes through* the packet engines." Claim Construction Order, Dkt. 162 at 33. In other words, some incoming packets could be dropped at the packet engines, but all incoming packets must be operated on by the packet engines.

The disclosures in the patent specification likewise confirms that while packets may be dropped by the packet engine, all "incoming packets" that enter the switch are passed by the switch

[redacted]

to the packet engine for processing. See, e.g., '436 Patent at 11:9-11 ("In one embodiment, **all incoming packets** to security processor 104 **may be initially processed by one of packet engines**."), 20:10-16 ("Regardless of destination, whether, for example, it is to streaming interface 200, host interface 206, control processor 212, or a loop through a packet engine 228, **all packet data preferably flows to a packet engine 228** and then to a corresponding cryptographic core 232.").

The Asserted Patents do not cover a system where "incoming packets" received by the switch are dropped by an intervening component before they reach the packet engine(s) for processing. Such a reading is excluded by the claim language, the Court's explanations at claim construction, and it is not supported by any specification disclosures.

2. *Some "Incoming Packets" are dropped before reaching the accused packet engines in the PA-5430.*

The relevant functionalities of the PA-5430 are not disputed. [redacted]

[redacted]

[redacted]

which is inconsistent with the Asserted Claims and the Court's claim construction explanation thereof, and for this reason no reasonable juror could conclude that the PA-5430 infringes any Asserted Claim. PAN therefore respectfully asks the Court to enter a finding of non-infringement.

B. PAN is entitled to summary judgment that the PA-5430 does not directly infringe the Asserted Claims because the PA-5430 is not configured to perform decryption as sold.

As explained below, each Asserted Claim requires "hardware, or a combination of hardware and software, that is configured to perform" decryption processing. The PA-5430 is not so configured as sold. Accordingly, the PA-5430 does not directly infringe any Asserted Claim.

1. Every Asserted Claim requires a "cryptographic core" configured to "provide encryption and decryption processing."

Starting with the language of the claims, each Asserted Claim requires a "cryptographic core, coupled to the packet engine and receiving the incoming packets … and communicating the outgoing packets … to provide encryption and decryption processing for packets." '436 Patent, Claim 1. The Court construed the term "cryptographic core" to mean "hardware, or a combination of hardware and software, that is ***configured to*** perform cryptographic processing." Dkt. 162, at 42 (emphasis added); Dkt. 190. Accordingly, in order to directly infringe the Asserted Claims, the cryptographic core must be "hardware, or a combination of hardware and software," that is actually "***configured to***" "provide encryption and decryption processing" for the received and communicated packets.

[redacted]

The specific, required configuration of "hardware or combination of hardware and software" is also evident from the surrounding claim language. Each Asserted Claim[3] requires that the cryptographic core must be "coupled to" a "packet engine." Regardless of whether the components are "hardware" or a "combination of hardware and software," or whether that coupling reflects a physical or processing connection, that coupling must be present to "receiv[e] the incoming packets" and "communicat[e] the outgoing packets." If the coupling can merely be made to exist through later configuration, it does not necessarily infringe. Given the specifically claimed arrangement of the Asserted Claims and the Court's constructions, it is clear that the claimed "cryptographic core" component must actually be "configured to perform cryptographic processing."

This is consistent with Federal Circuit cases distinguishing apparatuses which are merely capable of performing a recited function and apparatuses that are specifically configured to perform a recited function. For example, in *Ball Aerosol*, the Federal Circuit held that "infringement occurs only if the accused product is configured with the [claimed configuration] and "[t]hat the [accused product] was reasonably capable of being put into the claimed configuration is ***insufficient*** for a finding of infringement." *See Ball Aerosol & Specialty Container, Inc. v. Ltd. Brands, Inc.*, 555 F.3d 984, 995 (Fed. Cir. 2009) (emphasis added). Similarly, in a case where a device could be operated in two modes, a non-infringing mode and an allegedly infringing mode, the Federal Circuit held that "[b]ecause the accused device can be used at any given time in a noninfringing manner, the accused device does not necessarily infringe[.]" *ACCO Brands, Inc. v. ABA Locks Mfrs. Co.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007); *see also id.* ("In order to prove direct infringement [by defendant], a patentee must either point to specific

3 Each Asserted Claim is an apparatus claim.

[redacted]

instances of direct infringement or show that the accused device necessarily infringes the patent in suit.").

Thus, to directly infringe the Asserted Claims, the PA-5430 as sold must be configured to perform decryption, as opposed to being merely capable of performing decryption.

2. The PA-5430 is not configured to perform decryption as sold.

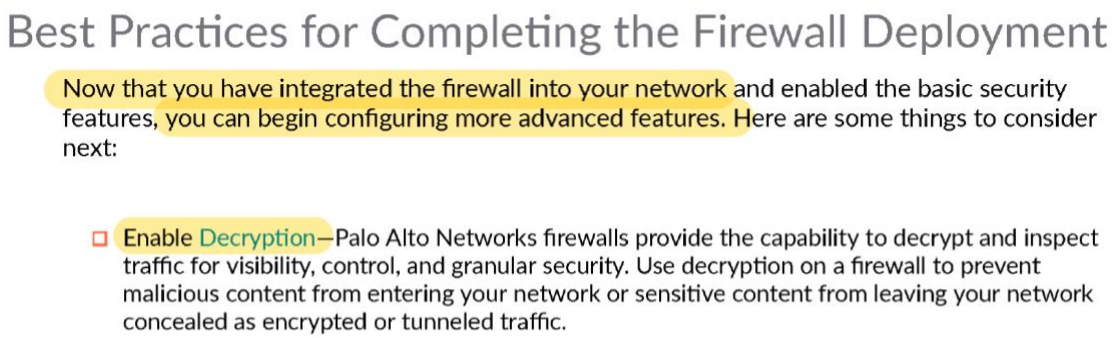
The alleged cryptographic core of the PA-5430 is not "configured to" "provide encryption and decryption processing" when sold by PAN and, therefore, PAN cannot directly infringe the Asserted Claims through sales of the PA-5430.

Dr. Smith alleges that the alleged "cryptographic core consists of the hardware and software used to encrypt and decrypt packets, performing at lease the functionality of the following modules in PAN_00022711" that are "accomplished via software calls by the PAN-OS software running on the processor." Ex. C, Smith Rep., Ex. G at ¶¶ 62-64. Even if true, the traffic decryption functionality is not enabled (i.e., not configured) on the PA-5430 when sold. Ex. A, Deng Decl., ¶ 10.

Instead, after receiving the PA-5430, the customer must first configure the PA-5430 to enable decryption processing. Ex. A, Deng Decl., ¶ 10; Ex. B, Lin Rebuttal Report, at ¶ 148. Mr. Deng—who has been employed at PAN since 2010 and is personally knowledgeable of the PA-5430 (Ex. A, Deng. Decl., ¶¶ 1–2)—has explained that [redacted] Ex. G, Deng Dep. Tr., at 45:20–46:13. In other words, the PA-5430 will not decrypt traffic until the customer configures the PA-5430 to do so.

[redacted]

This is further demonstrated in the PAN-OS Administrator's Guide. Ex. F, PAN-OS Administrator's Guide. Specifically, the PAN-OS Administrator's Guide contains the following page titled "Best Practices for Completing the Firewall Deployment" on page 62:



Best Practices for Completing the Firewall Deployment

Now that you have integrated the firewall into your network and enabled the basic security features, you can begin configuring more advanced features. Here are some things to consider next:

- Enable Decryption—Palo Alto Networks firewalls provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Use decryption on a firewall to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted or tunneled traffic.

Id. at 62 (annotated). As seen in annotated page 62, the PAN-OS Administrator's Guide establishes that *after* a user has "integrated the firewall into [a] network," the user can *then* "begin configuring more advanced features"—such as "[e]nabl[ing] [d]ecryption." *Id.* In other words, the PA-5430 running PAN-OS, is not configured to perform decryption until after the user integrates the firewall and specifically configures the device to perform decryption.

"[I]nfringement requires 'specific instances of direct infringement or that the accused device necessarily infringes the patent in suit.'" *Ball Aerosol*, 555 F.3d at 995 (quoting *ACCO Brands*, 501 F.3d at 1313). That the PA-5430 may be "reasonably capable of being put into the claimed configuration" "is insufficient for a finding of infringement." *Id.* Accordingly, because the PA-5430 is not configured to perform decryption and is not coupled to the packet engine when sold, there can be no direct infringement.

VII. CONCLUSION

For the foregoing reasons, there is no genuine dispute as to any material fact and PAN respectfully requests entry of summary judgment of non-infringement as to all Asserted Claims.

[redacted]

Dated: February 20, 2024

/s/ Mark C. Lang
Eric A. Buresh (KS Bar 19895)
Michelle L. Marriott (KS Bar 21784)
Mark C. Lang (KS Bar 26185)
Lydia C. Raw (admitted pro hac vice)
Nick R. Apel (admitted pro hac vice)
ERISE IP, P.A.
7015 College Blvd., Ste. 700
Overland Park, KS 66211
Tel: (913) 777-5600
Fax: (913) 777-5601
Eric.Buresh@eriseip.com
Michelle.Marriott@eriseip.com
Mark.Lang@eriseip.com
Lydia.Raw@eriseip.com
Nick.Apel@eriseip.com

Abran J. Kean (CO Bar 44660)
ERISE IP, P.A.
717 17th Street, Suite 1400
Denver, CO 80202
abran.kean@eriseip.com

Melissa Smith
Texas State Bar No. 24001351
melissa@gillamsmithlaw.com
GILLAM & SMITH, L.L.P.
303 South Washington Avenue
Marshall, Texas 75670
Telephone: 903-934-8450
Facsimile: 903-934-9257

Attorneys for Defendant Palo Alto Networks Inc.

[redacted]

CERTIFICATE OF SERVICE

The undersigned counsel hereby certifies that on February 20, 2024, a true and correct copy of the foregoing was served via email on all attorneys of record.

/s/ Mark C. Lang
Mark C. Lang

CERTIFICATE OF AUTHORIZATION TO FILE UNDER SEAL

I hereby certify that this document is filed under seal pursuant to the Protective Order approved and entered into this case.

/s/ Mark C. Lang
Mark C. Lang